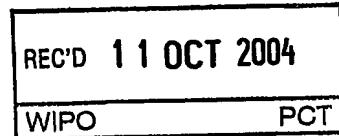


EP 04/08773

**Prioritätsbescheinigung über die Einreichung
einer Patentanmeldung**

Aktenzeichen: 103 36 404.8

Anmeldetag: 06. August 2003

Anmelder/Inhaber: Michael Adams, 50170 Kerpen/DE;
Ingo Büttner, 50171 Kerpen/DE.

Bezeichnung: Überwachungseinrichtung für Datenverarbeitungs-
anlagen

IPC: G 06 F 12/14

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 16. September 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Ebert

**PRIORITY
DOCUMENT**SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

Überwachungseinrichtung für Datenverarbeitungsanlagen

Die Erfindung betrifft eine Überwachungseinrichtung für eine Datenverarbeitungsanlage nach dem Oberbegriff des Anspruchs 1, sowie ein Verfahren nach dem Oberbegriff des Anspruchs 25.

Überwachungseinrichtungen für Datenverarbeitungsanlagen wie z.B. Computer sind hinlänglich bekannt. Meist wird über Berechtigungsanfragen mit Username und Passwort versucht, einen unerlaubten Zugriff auf Datenspeichereinrichtungen zu verhindern.

In EP 0 276 450 A1 wird eine Datenschuttschaltung zur Sperrung der Übertragung von Signalen über einen Bus beschrieben. In einem Register werden Codeschlossdaten als Festwert gespeichert und mit Codeschlüsseldaten aus einer Dekodierschaltung kombiniert. Beim Vorliegen eines bestimmten Ergebnisses der Kombination wird die Leitung eines Busses freigeschaltet.

Nachteilig bei dieser Vorrichtung ist, dass die gesamte Schaltung in der zu schützenden Datenverarbeitungsanlage angeordnet ist. Für versierte Nutzer besteht daher die Möglichkeit die Datenverarbeitungsanlage missbräuchlich derart zu manipulieren, dass ein unberechtigter Zugriff auf die geschützten Medien trotzdem möglich ist.

Auch bei der gängigen Softwareverschlüsselung ist es möglich, den Schutz zu umgehen, indem sekundär, beispielsweise über ein anderes Betriebssystem, auf diese Software zugegriffen wird und entsprechende Codeschlüsseldaten ausgelesen werden.

Der Erfindung liegt daher die Aufgabe zugrunde, eine Überwachungseinrichtung der eingangs genannten Art sowie ein Überwachungsverfahren für die Datenverarbeitungsanlage zu schaffen, bei denen die oben genannten Nachteile behoben werden und eine Manipulation der Datenverarbeitungsanlage nicht oder zumindest unbemerkt nicht möglich ist.

Zur Lösung dieser Aufgabe dienen die Merkmale des Anspruchs 1.

Die Erfindung sieht in vorteilhafter Weise vor, dass an einer bootfähigen Schnittstelle der Datenverarbeitungsanlage nur eine einzige Datenspeichereinrichtung als mainboot-device angeschlossen ist, die frei booten kann, dass andere bootfähige Schnittstellen zunächst gesperrt sind, und dass eine Freigabe mindestens einer der über die Sperrschaltung gesperrten Schnittstellen von einer im Netzwerk entfernt angeordneten Datenverarbeitungsstelle ausgehend nach Autorisierung eines Zugangsberechtigten gegenüber der Datenverarbeitungsstelle über die Netzwerkverbindung erfolgt.

Bei einer derartigen Anordnung kann eine Datenverarbeitungsanlage, beispielsweise ein Computer, nur über eine einzige Datenspeichereinrichtung, beispielsweise eine Festplatte, booten, so dass eine Manipulation der Datenverarbeitungsanlage, beispielsweise durch die Installation eines neuen Betriebssystems über eine bootfähige Schnittstelle, nicht möglich ist. Ein Umgehen der Sperrschaltung, beispielsweise über eine Software, ist nicht möglich, da die Sperrung der bootfähigen Schnittstellen über einer hardwareseitige Schaltung vorgenommen ist, die nur von einer separaten entfernten Datenverarbeitungsstelle, wie z.B. einen Ser-

ver, freigegeben werden kann. Ein unautorisierter Zugriff auf die bootfähigen Schnittstellen und entsprechend auf an diesen Schnittstellen angeschlossenen Datenspeichereinrichtungen ist nicht möglich.

In einer bevorzugten Ausführungsform der Erfindung ist vorgesehen, dass die Sperrschaltung zur Sperrung der bootfähigen Schnittstellen über einen CMOS erfolgt. CMOS-Bausteine sind Standardbauteile in der Elektronik, einfach anzu-steuern und daher eine kostengünstige Ausführungsform der Sperrschaltung.

Gemäß einer Weiterbildung der Erfindung ist vorgesehen, dass die Sperrschaltung auf dem Motherboard integriert ist. Diese Ausführungsform ist vor allem bei neu zu erwerbenden Computern von Vorteil, weil dies eine kostengünstige Version ist, die keine weitere Schnittstelle, wie z.B. einen Kartensteckplatz, in Anspruch nimmt.

Alternativ kann die Sperrschaltung auch auf einer separaten Karte mit separater Schnittstelle, vorzugsweise eine PCI-Karte, angeordnet sein. Die Anordnung auf einer separaten Karte ist von Vorteil, da auf diese Weise ältere Computer einfach und kostengünstig nachgerüstet werden können.

In einer bevorzugten Weiterbildung der Erfindung enthält die Sperrschaltung einen Mikrocontroller. Durch den Einsatz eines Mikrocontrollers in der Sperrschaltung wird diese zur einer aktiven Schaltung, die beispielsweise auch von der Software der Datenverarbeitungsanlage angesprochen werden kann, so dass ein Schaltvorgang in die Sperrstellung der Sperrschaltung auch durch beispielsweise ein Abmelden eines Users an der Datenverarbeitungsanlage vonstatten gehen kann.

Vorzugsweise ist vorgesehen, dass die Sperrschaltung über eine Empfangsleitung der Netzwerkverbindung von der Datenverarbeitungsstelle gesteuert ist. Dadurch ist es nicht nötig, eine zusätzliche einzelne Leitung der Netzwerkverbindung, also

eine einzelne Kabelverbindung, zu verwenden, so dass alle Leitungen der Netzwerkverbindungen auch für Datenverkehr genutzt werden können.

Die Sperrschaltung kann eine Reset-Leitung besitzen. Über diese Reset-Leitung kann beispielsweise durch eine Tastenkombination an der Tastatur eine Sperrung der Sperrschaltung manuell herbeigeführt werden, oder bei der Ausführungsform mit einem Power-Reset durch Ausschalten des Computers die Sperrschaltung in den Sperrzustand geschaltet werden. Auch kann über die Reset-Leitung die oben angesprochene Softwaresteuerung des Mikrokontrollers vorgenommen werden.

Nach einer bevorzugten Weiterbildung der Erfindung ist vorgesehen, dass an mindestens einer bootfähigen Schnittstelle eine Alarmschaltung vorgesehen ist, die vorzugsweise an der Netzwerkverbindung angeschlossen ist und ein Alarmsignal über die Netzwerkverbindung senden kann, und die vorzugsweise an einem freien Masse-Port der Schnittstelle angeschlossen ist. Durch diese Alarmschaltung ist eine manuelle Manipulation an den Datenspeichereinrichtungen, die an den Schnittstellen angeschlossen sind, unbemerkt nicht möglich. Durch den Anschluss an die Netzwerkverbindung kann das Alarmsignal über diese gesendet werden und entsprechend an entfernter Stelle registriert werden. Die meisten Schnittstellen haben heutzutage freie, ungenutzte Masse-Ports, so dass bei einem Anschluss an diesen, die Schnittstelle in ihren eigentlichen Funktionen nicht verändert wird.

Gemäß einer Weiterbildung der Erfindung ist an einem Gehäuse der Datenverarbeitungsanlage eine Alarmschaltung, vorzugsweise mit einem Tastschalter, angeordnet, die vorzugsweise an die Netzwerkverbindung angeschlossen ist und ein Alarmsignal über die Netzwerkverbindung senden kann. Durch diese Gehäusesicherung wird verhindert, dass ein unbemerkter Zugriff auf die Hardware an der Datenverarbeitungsanlage vorgenommen werden kann. Da die Alarmschaltung an die Netzwerkverbindung angeschlossen ist, kann ein Alarmsignal an eine entfernte Stelle gesendet werden.

Bei einer Weiterbildung der Erfindung ist vorgesehen, dass an mindestens einer Steckverbindung für eine Tastatur und/oder einen universellen seriellen Port an der Datenverarbeitungsanlage einer Alarmschaltung, vorzugsweise mit einem Buchsenshalter angeordnet ist, die vorzugsweise an die Netzwerkverbindung angeschlossen ist und ein Alarmsignal über die Netzwerkverbindung senden kann. Durch die Anordnung dieser Alarmschaltung wird ein unbemerkter Zugriff auf einen universellen seriellen Port, beispielsweise einen USB, verhindert oder bei einer der Steckverbindung der Tastatur ein Zwischenschalten eines sogenannten Tastaturrekorders, der zum Ausspionieren von Passwörtern genutzt werden kann, verhindert. Durch den Anschluss an die Netzwerkverbindung kann bei unerlaubtem Zugriff über die Netzwerkverbindung ein Alarmsignal versendet und an entfernter Stelle registriert werden.

Die Netzwerkverbindung kann gegen unautorisierten Zugriff, wie beispielsweise ein Abziehen eines oder mehrerer Anschlusspins, über eine Alarmschaltung geschützt sein. Mit dieser Alarmschaltung wird registriert, wenn ein Manipulationsversuch an der Datenverarbeitungsanlage durch den Anschluss einer neuen Netzwerkverbindung, bzw. den Anschluss eines oder mehrerer Pins der Netzwerkverbindung, vorgenommen wird.

Vorzugsweise ist vorgesehen, dass eine oder mehrere der Alarmschaltungen an einem Sende-/ Empfangsleitungsstrang der Netzwerkverbindung, vorzugsweise an einzelnen Leitungen, angeschlossen ist. Wenn die Alarmschaltungen an dem Sende-/ Empfangsleitungsstrang der Netzwerkverbindung, also dem Teil der Verbindung, der für den Datenverkehr genutzt wird, können in Zukunft etwaige freie Netzwerkverbindungsteile für andere Zwecke genutzt werden. Durch den Anschluss an einzelne Leitungen kann bei der Registrierung eines Alarms eine Zuordnung zu der auslösenden Alarmschaltung vorgenommen werden, so dass beispielsweise sofort registriert werden kann, ob eine Festplatte entfernt wird. Entsprechend der Wichtigkeit der entdeckten Manipulation der Datenverarbeitungs-

anlagen können entsprechend unterschiedliche Alarmprogramme ausgelöst werden.

Bei einer ersten Ausführungsform der Erfindung sind die Alarmschaltungen überwiegend parallel geschaltet und zu einer Leitung zusammengefasst. Weiter ist vorgesehen, dass die zusammengefassten Alarmschaltungen über eine Sternverdrahtung und Spulen an zwei Leitungen der Netzwerkverbindungen angeschlossen sind, dass eine Alarmdetektierungseinrichtung über Spulen an die zweite Leitung der Netzwerkverbindung, entfernt von der Datenverarbeitungsanlage, angeschlossen ist und dass ein Alarmübertragungsweg über eine Phantomleitung gebildet wird. Bei dieser Ausführungsform der Erfindung ist ein schaltungsseitig geringer Aufwand vorzunehmen. Durch den Übertragungsweg über eine Phantomleitung werden nur zwei einzelne Leitungen der Netzwerkverbindungen genutzt. Durch die Anordnung der Spulen wird das standardmäßige Hochfrequenzsignal der Netzwerkverbindung gegenüber den Alarmschaltungen und der Alarmdetektierungseinrichtung abgeblockt. Dies ist vorteilhaft, weil ein eindeutiges Signal zwischen der Alarmschaltung und der Alarmdetektierungseinrichtung übermittelt werden kann. Durch die Anordnung der Widerstände an den einzelnen Alarmschaltungen kann beispielsweise durch die Variation der Größe der Widerstände, trotz der Übertragung des Alarmsignals über nur zwei Leitungen, eine klare Zuordnung des Alarmsignals vorgenommen werden, da die unterschiedlichen Widerstände ein unterschiedliches Alarmsignal hervorrufen.

In einer alternativen Ausführungsform der Erfindung sind in den einzelnen Leitungen der Netzwerkverbindungen jeweils mindestens zwei Kondensatoren angeordnet. Zwischen den Kondensatoren sind die Alarmschaltungen über eine Sternverdrahtung an die einzelnen Leitungen der Netzwerkverbindung angeschlossen. Weiter ist vorzugsweise vorgesehen, dass die Alarmdetektierungseinrichtung entfernt von der Datenverarbeitungsanlage über eine Sternverdrahtung jeweils zwischen den Kondensatoren an die Einzelleitungen der Netzwerkverbindung angeschlossen ist. Diese Anordnung hat zum Vorteil, dass eine Übertragung eines

Alarmsignals mit Gleichstrom erfolgen kann. Durch die Trennung der einzelnen Netzwerkverbindungsleitungen mit Kondensatoren ist eine ungehinderte Alarmsignalübertragung zwischen Alarmschaltungen und der Alarmdetektierungseinrichtung möglich, die gegenüber der weiteren Datenübertragung der Netzwerkverbindung separiert ist, ohne die Datenübertragung über die Netzwerkverbindung zu behindern. Durch die entfernte Anordnung der Alarmdetektierungseinrichtung von der Datenverarbeitungsanlage ist es möglich, dass ein Alarm detektiert werden kann, ohne dass die Person, die die Manipulation vornimmt, den ausgelösten Alarm bemerkt. Es besteht somit die Möglichkeit bei Alarmauslösung rechtzeitig die erforderlichen Maßnahmen zu ergreifen, um die Person an der Manipulation zu hindern.

Es ist vorgesehen, dass eine Alarmdetektierung über eine Überwachung eines Ruhestromes erfolgt, der an den Alarmschaltungen angelegt ist. Dies ermöglicht eine kostengünstige Lösung der Alarmsignalübertragung und über die Verwendung von unterschiedlich großen Widerständen in den Alarmschaltungen auch die Möglichkeit einer genauen Zuordnung des entsprechenden Alarmsignal, auch wenn die Anzahl der zu überwachenden Schnittstellen oder Datenspeichereinrichtungen größer als die Anzahl der einzelnen Leitungen der Netzwerkverbindungen ist. Ferner können durch die Nutzung des Ruhestromes die vorhandenen Datenübertragungswege genutzt werden, da diese die Daten hochfrequent übertragen und vom Ruhestrom nicht beeinflusst werden.

In einer besonders bevorzugten Weiterbildung der Erfindung wird der Ruhestrom dynamisch über einen Zufallsgenerator erzeugt und einerseits zu den Alarmschaltungen und andererseits einer parallelen Referenzschaltung zugeführt und dann an einer Vergleichsstelle entfernt von der Datenverarbeitungsanlage überwacht. Dies ist von Vorteil, weil auf diese Weise die Höhe des Ruhestromes an der Datenverarbeitungsanlage nicht bekannt ist bzw. nicht ermittelt werden kann und somit eine Manipulation der Alarmschaltung durch externe Anlegung eines Ruhestromes der gleichen Höhe nicht möglich ist.

In einer alternativen Weiterbildung der Erfindung ist eine oder mehrere der Alarmschaltungen an einem separaten Leitungsstrang der Netzwerkverbindung, vorzugsweise jeweils an einzelne Leitungen angeschlossen. Ferner ist vorgesehen, dass eine Alarmedetektierungseinrichtung entfernt von der Datenverarbeitungsanlage an einzelne Leitungen des separaten Leitungsstranges der Netzwerkverbindung angeschlossen ist. Den Alarmübertragungsweg somit über einen separaten Leitungsstrang der Netzwerkverbindung zu leiten, hat den Vorteil, dass es zu keiner wechselseitigen Störung der Alarmsignale und des Datenverkehrs kommen kann. Durch die Anordnung der Alarmedetektierungseinrichtung entfernt von der Datenverarbeitungsanlage ist eine Manipulation der Alarmedetektierungseinrichtung nicht möglich und ein Alarm kann unbemerkt von dem Alarmverursacher ausgelöst werden.

In dieser alternativen Ausführungsform erfolgt eine Alarmedetektierung durch die Überwachung eines über die Netzwerkverbindung der Alarmschaltungen angelegten Ruhestromes.

Bei einer speziellen Ausführungsform mit einer besonders hohen Sicherheitsstufe bewirkt ein ausgelöster Alarm über eine Vorrichtung, beispielsweise ein Bolzenschussgerät, eine mechanische Zerstörung von mindestens einem zugriffgeschützten Datenträger der Datenverarbeitungsanlage. Besonders vertrauliche Daten werden über diese Vorrichtung nicht konstruierbar zerstört, so dass diese bei Manipulation der Datenverarbeitungsanlage mit hoher krimineller Energie, beispielsweise einem Diebstahl der gesamten Datenverarbeitungsanlage, für die entsprechende Person unbrauchbar wird.

Vorzugsweise ist vorgesehen, dass eine Schaltung zum manuellen Auslösen des Alarms an mindestens einer der Alarmschaltungen angeordnet ist. Diese Schaltung kann beispielsweise einen Handschalter beinhalten. Ein Alarm und somit eine Sperrung der Schnittstellen und/oder eine mechanische Zerstörung eines

Datenträgers können somit auch manuell auf Befehl des autorisierten Benutzers ausgelöst werden.

Die Erfindung betrifft weiter ein Verfahren zur Überwachung einer Datenverarbeitungsanlage in einem Netzwerk mit Netzwerkverbindungen zum Schutz vom Datenspeicher und/oder Datenübertragungseinrichtungen der Datenverarbeitungsanlage vor unautorisiertem Zugriff, bei der bei einem Bootvorgang nur auf eine einzige Datenspeichereinrichtung an einer bootfähigen Schnittstelle der Datenverarbeitungsanlage zugegriffen werden kann, wobei andere bootfähige Schnittstellen zunächst gesperrt sind und wobei eine Freigabe der gesperrten Schnittstellen von einer im Netzwerk entfernt angeordneten Datenverarbeitungsstelle ausgehend nach Autorisierung eines Zugangsberechtigten gegenüber der Datenverarbeitungsstelle über die Netzwerkverbindung erfolgt.

Die Datenverarbeitungsstelle kann hierbei die Sperrung der Schnittstellen über eine Empfangsleitung der Netzwerkverbindung und eine Sperrschaltung steuern.

Vorzugsweise ist vorgesehen, dass die Sperrung der bootfähigen Schnittstellen nach einem Ausschalten der Datenverarbeitungsanlage und/oder dem Abmelden des Benutzers an der Datenverarbeitungsanlage über ein Reset in einen Sperrzustand zurückkehrt.

Ein Entfernen einer Datenspeichereinrichtung und/oder einer Datenübertragungseinrichtung einer Datenverarbeitungsanlage sowie ein Öffnen eines Gehäuses der Datenverarbeitungsanlage kann einen Alarm an einer entfernten Alarmedetektierungseinrichtung auslösen.

Der Alarm kann auch manuelle, beispielsweise über einen Schalter, ausgelöst werden.

Vorzugsweise ist vorgesehen, dass ein ausgelöster Alarm eine mechanische Zerstörung von mindestens einem zugriffsgeschützten Datenträger der Datenverarbeitungsanlage bewirkt.

Mit diesem erfindungsgemäßen Verfahren können die oben genannten Vorteile verwirklicht werden.

Im folgenden wird unter Bezugnahme auf die Zeichnungen einige Ausführungsbeispiele der Erfindung näher erläutert:

Es zeigen:

Figur 1 eine Schaltskizze der erfindungsgemäßen Überwachungseinrichtung, bei der der Übertragungsweg eines Alarmsignals über eine Phantomleitung erfolgt,

Figur 2 eine Schaltskizze einer alternativen Ausführungsform der erfindungsgemäßen Überwachungseinrichtung, bei der die Übertragung des Alarmsignals über einzelne Leitungen der Netzwerkverbindung erfolgt,

Figur 3 eine Weiterbildung des Ausführungsbeispiels aus Figur 2, bei der zusätzlich eine Schaltung zur Erzeugung eines dynamischen Ruhestromes an die Alarmdetektierung angeschlossen ist,

Figur 4 eine Schaltskizze einer weiteren Ausführungsform der erfindungsgemäßen Überwachungseinrichtung, bei der der Übertragungsweg eines Alarmsignals durch separate Leitungen der Netzwerkverbindung gebildet sind.

Eine Überwachungseinrichtung 1 für eine Datenverarbeitungsanlage 2 ist als Schaltung in Figur 1 dargestellt. Die Schaltung kann als separate Einsteckkarte oder als Schaltung direkt auf dem Motherboard der Datenverarbeitungsanlage 2 verwirklicht sein.

An einer bootfähigen Schnittstelle 8, beispielsweise einer IDE-Schnittstelle, ist nur eine einzige Datenspeichereinrichtung 9, beispielsweise eine Festplatte, angeschlossen. Bei anderen bootfähigen Schnittstellen 10, 12, 14, beispielsweise eine weitere IDE, eine Floppy, eine USB, oder eine Firewire-Schnittstelle, ist jeweils eine sperrfähige Schalteinrichtung 18, beispielsweise ein CMOS, integriert. Die Schnittstelle 14 kann eine oder mehrere Schnittstellen umfassen und ist nicht dargestellt. In Figur 1, ist dies nur für die Schnittstellen 10 und 12 dargestellt. Selbstverständlich kann in ähnlicher Weise auch eine Schalteinrichtung in der nicht dargestellten Schnittstelle 14 integriert sein. Die Schalteinrichtungen 18 werden über einen Mikrokontroller 20 angesteuert. Dieser Mikrokontroller 20 ist über die Empfangsleitungen 22 einer Netzwerkverbindung 4 mit einer entfernten nicht dargestellten Datenverarbeitungsstelle 16, beispielsweise einem zentralen Server, verbunden. Ferner ist an den Mikrokontroller eine Reset-Leitung 24 angeschlossen. Die Sperrschalteinrichtungen 18 bilden zusammen mit dem Mikrokontroller die Sperrschaltung 6. Selbstverständlich kann die Sperrschaltung 6 auch als passive Schaltung ohne Mikrokontroller verwirklicht werden. Bei dem Bootvorgang eines Computers befindet sich die gesamte Sperrschaltung 6 zunächst in einer Sperrstellung. Der Computer kann nur von der Datenspeichereinrichtung 9, die als mainboot-device angeschlossen ist, gebootet werden. Nach Autorisierung eines Zugangsberechtigten gegenüber der Datenverarbeitungsstelle 16 über die Netzwerkverbindung 4 wird über die Netzwerkverbindung 4 ein Signal von der Datenverarbeitungsstelle 16 an den Mikrokontroller 20 gesendet, so dass die Sperrschalteinrichtungen 18 der bootfähigen Schnittstellen 10, 12, 14 freigeschaltet werden und der Zugangsberechtigte Zugriff auf alle Datenspeichereinrichtungen der Datenverarbeitungsanlage 2 hat. Selbstverständlich ist es auch möglich, nur einzelne der Schnittstellen 10, 12, 14 freizugeben, so dass ein Zu-

gangsberechtigter je nach Berechtigungsart beispielsweise nur auf eine Festplatte zugreifen kann, jedoch nicht auf einen CD-Brenner.

Der bisher beschriebene Teil der Überwachungseinrichtung ist bei jedem dargestellten Ausführungsbeispiel der Erfindung identisch.

In einem freien Port beispielsweise einem freien Masse-Port einzelner oder aller Schnittstellen 8, 10, 12, 14 sind Alarmschaltungen 28, 30, 32, 34 angeschlossen. Diese sind über parallelgeschaltete Widerstände 40 zu einer Leitung 42 zusammengefasst.

Über weitere Alarmschaltungen 36, 38 ist das Gehäuse der Datenverarbeitungsanlage 2 mit Tastschaltern oder beispielsweise die Tastaturverbindung mit Buchsensaltern gesichert. Die Buchsensalter lösen bei einer Kabelsteckverbindung einen Schaltvorgang beim Abziehen oder Einstecken des Kabels aus. Die Alarmschaltungen 36, 38 sind über ebenfalls parallelgeschaltete Widerstände an die Leitung 42 angeschlossen (nicht dargestellt).

Die Netzwerkverbindung 4 besteht zumindest aus vier einzelnen Leitungen, die zusammengefasst den Empfangs-/Sendeleitungsstrang 26a bilden, wobei zwei Leitungen Empfangsleitungen 22 sind. Selbstverständlich kann die Netzwerkverbindung 4 auch noch mehr Leitungen beinhalten, wie beispielsweise in Figur 4 dargestellt ist, mit einem weiteren separaten Leitungsstrang 26b.

Die Leitung 42 ist über zwei Spulen 48 an die beiden Empfangsleitungen 22 der Netzwerkverbindung 4 angeschlossen. Entfernt von der Datenverarbeitungsanlage 2 ist eine Alarmedetektierungseinrichtung 46 über zwei Spulen 48 an die Empfangsleitungen 22 der Netzwerkverbindung 4 angeschlossen. Die Spulen 48 dienen zur Entkopplung des Hochfrequenzsignals, das über die Netzwerkverbindung 4 gesendet wird. Von der Datenverarbeitungsanlage 46 ist ein Ruhestrom über die so gebildete Phantomleitung an die Alarmschaltungen 28-38 angelegt. Bei

Unterbrechung eines der Alarmschaltungen beispielsweise durch Abziehen einer Schnittstelle, einer Datenspeichereinrichtung oder einer gesicherten Steckverbindung, ändert sich der Ruhestrom. Diese Veränderung wird von der Alarmdetektierungseinrichtung 46 registriert und ein Alarm wird ausgelöst.

Durch den Einsatz von unterschiedlichen Widerständen in den Alarmschaltungen 28-38, kann von der Alarmdetektierungseinrichtung 46 die Quelle des Alarms detektieren, da durch den Wegfall eines Widerstandes 40 einer bestimmten Größe der Ruhestrom in einem bestimmten Maße verändert wird.

Figur 2 zeigt eine alternative Ausführungsform der Erfindung. Die Alarmschaltungen 28, 30, 32 sind einzeln jeweils an eine Leitung 4a, 4b, 4c der Netzwerkverbindung 4 angeschlossen. Die Alarmschaltungen 34, 36, 38, die in dieser Figur nicht dargestellt sind, sind entweder jeweils einzeln an eine Leitung 4a-4d der Netzwerkverbindung 4 angeschlossen (in dieser Zeichnung nicht dargestellt) oder sind zu einer Leitung zusammengefasst, die an die Leitung 4d der Netzwerkverbindung 4 angeschlossen ist. Jede Alarmschaltung beinhaltet eine Spule 48, die zum Abschirmen gegen das Hochfrequenzsignal der Netzwerkverbindung 4 dient. In jeder der Alarmschaltungen 28, 30, 32, 34, 36, 38 ist jeweils mindestens ein Widerstand 40 angeordnet, der als Last in diesen Schaltungen dient. Durch Abziehen beispielsweise einer Festplatte wird die entsprechende Alarmschaltung unterbrochen. Durch den Wegfall des Widerstandes ergibt sich eine Änderung in dem Ruhestrom.

Entfernt von der Datenverarbeitungsstelle 2 ist eine Alarmdetektierungseinrichtung 46 über Spulen 48 jeweils an einzelne Leitungen 4a, 4b, 4c, 4d der Netzwerkverbindung 4 angeschlossen. Jeweils zwei der Kondensatoren 50 sind derart in den einzelnen Leitungen 4a, 4b, 4c, 4d der Netzwerkverbindung 4 angeordnet, dass ein direkter Verbindungsweg zwischen den Alarmschaltungen 28-38 und der Alarmdetektierungseinrichtung 46 verbleibt und diese Leitungsweg gegenüber dem übrigen Teil der Netzwerkverbindungen 4 separiert ist. Die Verbindungslei-

tungen zwischen Alarmedetektierungseinrichtung 46 und der Netzwerkverbindung 4 können auch in einer nicht dargestellten Ausführungsform zu einer Leitung zusammengeschlossen werden. In diesem Fall ist es sinnvoll, dass die Widerstände 40 von unterschiedlicher Größe sind, so dass jeweils ein Wegfall dieser Widerstände zu einer unterschiedlichen Veränderung des Ruhestromes führt und somit ein ausgelöster Alarm einer bestimmten Alarmschaltung zugeordnet werden kann. Die Alarmedetektierungseinrichtung 46 beinhaltet eine Stromquelle, die einen Ruhestrom über die Netzwerkverbindung 4 an die Alarmschaltungen 28, 30, 32, 34, 36, 38 anlegt.

Figur 3 stellt eine erfindungsgemäße Überwachungseinrichtung dar, bei der die Alarmedetektierung über einen dynamisch geregelten Ruhestrom erfolgt. Die Anschlussleitungen der Alarmedetektierungseinrichtung 46 an die Netzwerkverbindung 4 umfassen Spulen 48 zur Entkopplung des Hochfrequenzsignals in der Netzwerkverbindung 4 und werden zu einer Leitung zusammengefasst. Ein Zufallsgenerator 52 ist mit einer Stromquelle 58 verbunden, die einen dynamischen Ruhestrom erzeugt und an die Netzwerkverbindung 4 und über diese an die Alarmschaltungen 28, 30, 32, 34, 36 anlegt. Eine Referenzschaltung 54 ist ebenfalls an die Stromquelle angeschlossen. An einer Vergleichsstelle 56 wird der an die Referenzleitung 54 und an die Alarmschaltungen angelegter Ruhestrom verglichen. Die Vergleichsstelle 56 registriert Veränderungen des dynamischen Ruhestroms, der an die Alarmschaltung angelegt ist, gegenüber dem Ruhestrom, der an die Referenzschaltung angelegt ist, und löst entsprechend einen Alarm aus.

Figur 4 zeigt eine weitere alternative Ausführungsform der Erfindung. Bei dieser Ausführungsform wird das Alarmsignal über einen separaten Leitungsstrang 26b der Netzwerkverbindung 4 übertragen. Die Alarmschaltungen 28, 30, 32 sind an einzelne Leitungen 4e-4g der Netzwerkverbindung 4 angeschlossen. Die Alarmschaltung 34, 36, 38 können in einzelnen Leitungen 4e bis 4h der Netzwerkverbindung 4 angeschlossen sein (nicht dargestellt) oder zu einer Leitung zusammengefasst an die einzelnen Leitungen 4h der Netzwerkverbindung 4 an-

geschlossen sein. Entfernt von der Datenverarbeitungsanlage 2 ist eine Alarmedektierung 46 an die einzelnen Leitungen 4e bis 4h der Netzwerkverbindung 4 angeschlossen. Entsprechend den vorangegangenen Ausführungsbeispielen führt von der Alarmedektierungseinrichtung ein Ruhestrom über die Netzwerkverbindung 4 an die Alarmschaltungen 28, 30, 32, 34, 36 angelegt. Die einzelnen Verbindungsleitungen der Alarmedektierung zu den einzelnen Leitungen 4e bis 4h der Netzwerkverbindung können auch zu einer Leitung zusammengefasst sein, die diese dann mit der Alarmedektierungseinrichtung 46 verbindet. Die in Figur 4 dargestellten Spulen 48 sind nicht erforderlich, wenn über den separaten Leitungsstrang 26b nur das Alarmsignal übertragen wird.

Bei allen beschriebenen Ausführungsformen wird an die Alarmschaltungen 28-38 nur ein Pol des Ruhestromes angeschlossen. Der andere Pol wird durch die Masse gebildet.

Selbstverständlich ist die Erfindung nicht auf die dargestellten Ausführungsbeispiele beschränkt. Es ist beispielsweise möglich eine Alarmedektierungseinrichtung 46 mit dynamischer Ruhestromregelung wie in Figur 3 dargestellt, mit der Phantomleitung als Alarmübertragungsweg wie in Figur 1 dargestellt zu kombinieren. Auch ist es möglich die Alarmschaltungen 28-38 in unterschiedlicher Paarung zu einzelnen Leitungen zusammenzuschließen, die dann entsprechend an die Netzwerkverbindung 4 angeschlossen sind. Die Sicherung weiterer Komponenten der Datenverarbeitungsanlage ist auf ähnliche Weise wie dargestellt möglich. Ferner können selbstverständlich die unterschiedlichen Merkmale der einzelnen Ausführungsbeispiele miteinander kombiniert werden.

Patentansprüche

1. Überwachungseinrichtung (1) für eine Datenverarbeitungsanlage (2) in einem Netzwerk mit Netzwerkverbindungen (4) zum Schutz von Datenspeicher- und/oder Datenübertragungseinrichtungen der Datenverarbeitungsanlage vor unautorisiertem Zugriff, wobei die Datenverarbeitungsanlage eine Sperrschaltung (6) von Schnittstellen (8, 10, 12, 14) aufweist, dadurch gekennzeichnet, dass an einer bootfähigen Schnittstelle (8) der Datenverarbeitungsanlage (2) nur eine einzige Datenspeichereinrichtung (9) als mainboot-device angeschlossen ist, die frei booten kann, dass andere bootfähige Schnittstellen (10, 12, 14) zunächst gesperrt sind, und dass eine Freigabe mindestens einer der über die Sperrschaltung (6) gesperrten Schnittstellen (10, 12, 14) von einer im Netzwerk entfernt angeordneten Datenverarbeitungsstelle (16) ausgehend nach Autorisierung eines Zugangsberechtigten gegenüber der Datenverarbeitungsstelle (16) über die Netzwerkverbindung (4) erfolgt.
2. Überwachungseinrichtung nach Anspruch 1, dadurch gekennzeichnet, dass die Sperrschaltung (6) zur Sperrung der bootfähigen Schnittstellen (10, 12, 14) über einen CMOS (18) erfolgt.
3. Überwachungseinrichtung nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass die Sperrschaltung (6) auf dem Motherboard integriert ist.
4. Überwachungseinrichtung nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass die Sperrschaltung (6) auf einer separaten Karte mit separater Schnittstelle, vorzugsweise eine PCI-Karte, angeordnet ist.

5. Überwachungseinrichtung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Sperrschaltung (6) einen Microcontroller (20) enthält.
6. Überwachungseinrichtung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Sperrschaltung (6) über eine Empfangsleitung (22) der Netzwerkverbindung (4) von der Datenverarbeitungsstelle (16) gesteuert ist.
7. Überwachungseinrichtung nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass die Sperrschaltung (6) eine Reset-Leitung (24) besitzt, vorzugsweise einen Power-Reset.
8. Überwachungseinrichtung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass an mindestens einer bootfähigen Schnittstellen (8, 10, 12, 14) eine Alarmschaltung (28, 30, 32, 34) angeschlossen ist, die vorzugsweise mit der Netzwerkverbindung (4) verbunden ist und ein Alarmsignal über die Netzwerkverbindung senden kann, sowie vorzugsweise an einem freien Masseport der Schnittstelle (8, 10, 12, 14) angeschlossen ist.
9. Überwachungseinrichtung nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass an einem Gehäuse der Datenverarbeitungsanlage (2) eine Alarmschaltung (36), vorzugsweise mit einem Tastschalter, angeordnet ist, die vorzugsweise an die Netzwerkverbindung (4) angeschlossen ist und ein Alarmsignal über die Netzwerkverbindung (4) senden kann.
10. Überwachungseinrichtung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass an mindestens einer Steckverbindung für eine Tastatur und/oder einen universellen seriellen Port an der Datenverarbeitungsanlage (2) eine Alarmschaltung (38), vorzugsweise mit einem Buchsenshalter, an-

geordnet ist, die vorzugsweise an die Netzwerkverbindung (4) angeschlossen ist und ein Alarmsignal über die Netzwerkverbindung (4) senden kann.

11. Überwachungseinrichtung nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass die Netzwerkverbindung (4) gegen unautorisierten Zugriff, wie beispielsweise ein Abziehen eines oder mehrerer Anschluss-Pins, über eine Alarmschaltung geschützt ist.
12. Überwachungseinrichtung nach einem der Ansprüche 8 bis 11, dadurch gekennzeichnet, dass eine oder mehrere der Alarmschaltungen (28, 30, 32, 34, 36, 38) an einem Sende-Empfangsleitungsstrang (26a) der Netzwerkverbindung (4), vorzugsweise an einzelnen Leitungen (4a-d), angeschlossen ist.
13. Überwachungseinrichtung nach Anspruch 12, dadurch gekennzeichnet, dass die Alarmschaltungen (28, 30, 32, 34, 36, 38) über Widerstände (40) parallel geschaltet und zu einer Leitung (42) zusammengefasst sind.
14. Überwachungseinrichtung nach Anspruch 13, dadurch gekennzeichnet, dass die zusammengefassten Alarmschaltungen (28, 30, 32, 34, 36, 38) über eine Sternverdrahtung und Spulen (44) an zwei Leitungen der Netzwerkverbindung (4) angeschlossen sind, dass eine Alarmdetektierungseinrichtung (46) über Spulen (48) an die zwei Leitungen der Netzwerkverbindung (4) entfernt von der Datenverarbeitungsanlage (2) angeschlossen ist und dass ein Alarmübertragungsweg über eine Phantomleitung gebildet wird.
15. Überwachungseinrichtung nach einem der Ansprüche 8 bis 12, dadurch gekennzeichnet, dass in einzelnen Leitungen (4a-d) der Netzwerkverbindung (4) jeweils mindestens zwei Kondensatoren (50) angeordnet sind.

16. Überwachungseinrichtung nach Anspruch 15, dadurch gekennzeichnet, dass die Alarmschaltungen (28, 30, 32, 34, 36, 38) über eine Sternverdrahtung zwischen den Kondensatoren (50) an die einzelnen Leitungen (4a-d) der Netzwerkverbindung (4) angeschlossen sind.
17. Überwachungseinrichtung nach einem der Ansprüche 15 oder 16, dadurch gekennzeichnet, dass eine Alarmdetektierungseinrichtung (46) entfernt von der Datenverarbeitungsanlage (2) über eine Sternverdrahtung jeweils zwischen den Kondensatoren (50) an die einzelnen Leitungen (4a-d) der Netzwerkverbindung (4) angeschlossen ist.
18. Überwachungseinrichtung nach Anspruch 14 oder 17, dadurch gekennzeichnet, dass eine Alarmdetektierung über eine Überwachung eines Ruhestromes erfolgt, der über die Netzwerkverbindung an die Alarmschaltungen (28, 30, 32, 34, 36, 38) angelegt ist.
19. Überwachungseinrichtung nach Anspruch 18, dadurch gekennzeichnet, dass der Ruhestrom dynamisch über einen Zufallsgenerator (52) erzeugt ist, dass der Ruhestrom einerseits der Alarmschaltungen (28, 30, 32, 34, 36, 38) und andererseits einer parallele Referenzschaltung (54) zugeführt ist und dass die parallel angelegten Ruhestrome an einer Vergleichsstelle (56) überwacht werden.
20. Überwachungseinrichtung nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, dass eine oder mehrere der Alarmschaltungen (28, 30, 32, 34, 36, 38) an einem separaten Leitungsstrang (26b) der Netzwerkverbindung (4), vorzugsweise jeweils an einzelnen Leitungen (4e-h), angeschlossen ist.
21. Überwachungseinrichtung nach Anspruch 20, dadurch gekennzeichnet, dass eine Alarmdetektierungseinrichtung (46) entfernt von der Datenverarbei-

tungsanlage (2) an den einzelnen Leitungen (4e-h) des separaten Leitungsstranges (26b) der Netzwerkverbindung (4) angeschlossen ist.



22. Überwachungseinrichtung nach Anspruch 21, dadurch gekennzeichnet, dass eine Alarmdetektierung durch die Überwachung eines über die Netzwerkverbindung an die Alarmschaltungen (28, 30, 32, 34, 36, 38) angelegten Ruhestromes erfolgt.
23. Überwachungseinrichtung nach einem der Ansprüche 8 bis 22, dadurch gekennzeichnet, dass ein ausgelöster Alarm über eine Vorrichtung, beispielsweise ein Bolzenschußgerät, eine mechanische Zerstörung von mindestens einem zugriffsgeschützten Datenträger der Datenverarbeitungsanlage (2) bewirkt.
24. Überwachungseinrichtung nach einem der Ansprüche 8 bis 23, dadurch gekennzeichnet, dass eine Schaltung zum manuellen Auslösen des Alarms, beispielsweise mit einem Handschalter, an mindestens einer der Alarmschaltungen (28, 30, 32, 34, 36, 38) angeordnet ist.
25. Verfahren für die Überwachung einer Datenverarbeitungsanlage (2) in einem Netzwerk mit Netzwerkverbindungen (4), zum Schutz von Datenspeicher- und/oder Datenübertragungseinrichtungen der Datenverarbeitungsanlage (2) vor unautorisiertem Zugriff,

dadurch gekennzeichnet,

dass bei einem Bootvorgang nur auf eine einzige Datenspeichereinrichtung an einer bootfähigen Schnittstelle (8) der Datenverarbeitungsanlage (2) zugegriffen werden kann,

dass andere bootfähige Schnittstellen (10, 12, 14) zunächst gesperrt sind, und

dass eine Freigabe der gesperrten Schnittstellen (10, 12, 14) von einer im Netzwerk entfernt angeordneten Datenverarbeitungsstelle (16) ausgehend, nach Autorisierung eines Zugangsberechtigten gegenüber der Datenverarbeitungsstelle (2) über die Netzwerkverbindung (4) erfolgt.

- 
26. Verfahren nach Anspruch 25, dadurch gekennzeichnet, dass die Sperrung der Schnittstellen (10, 12, 14) über eine Empfangsleitung der Netzwerkverbindung (4) und eine Sperrschaltung (6) von der Datenverarbeitungsstelle (16) gesteuert wird.
27. Verfahren nach einem der Ansprüche 25 oder 26, dadurch gekennzeichnet, dass die Sperrung der bootfähigen Schnittstellen (10, 12, 14) nach einem Ausschalten der Datenverarbeitungsanlage (2) und/oder dem Abmelden des Benutzers an der Datenverarbeitungsanlage (2) über ein Reset in einen Sperrzustand zurückgesetzt wird.
- 
28. Verfahren nach einem der Ansprüche 25 bis 27, dadurch gekennzeichnet, dass ein Alarm an einer entfernten Alarmdetektierungseinrichtung (46) durch ein Entfernen einer Datenspeichereinrichtung und/ oder einer Datenübertragungseinrichtung der Datenverarbeitungsanlage (2) sowie durch ein Öffnen eines Gehäuses der Datenverarbeitungsanlage (2) ausgelöst wird.
29. Verfahren nach Anspruch 28, dadurch gekennzeichnet, dass der Alarm manuell, beispielsweise über einen Schalter, ausgelöst werden kann.
30. Verfahren nach einem der Ansprüche 28 oder 29, dadurch gekennzeichnet, dass eine mechanische Zerstörung von mindestens einem zugriffsgeschützten Datenträger der Datenverarbeitungsanlage (2) durch einen ausgelösten Alarm bewirkt wird.

Zusammenfassung

Bei einer Überwachungseinrichtung (1) für eine Datenverarbeitungsanlage (2) in einem Netzwerk mit Netzwerkverbindungen (4) zum Schutz von Datenspeicher- und/oder Datenübertragungseinrichtungen der Datenverarbeitungsanlage vor unautorisiertem Zugriff, wobei die Datenverarbeitungsanlage eine Sperrschaltung (6) von Schnittstellen (8, 10, 12, 14) aufweist, ist vorgesehen, dass an einer bootfähigen Schnittstelle (8) der Datenverarbeitungsanlage (2) nur eine einzige Datenspeichereinrichtung (9) als mainboot-device angeschlossen ist, die frei booten kann, dass andere bootfähige Schnittstellen (10, 12, 14) zunächst gesperrt sind, und dass eine Freigabe mindestens einer der über die Sperrschaltung (6) gesperrten Schnittstellen (10, 12, 14) von einer im Netzwerk entfernt angeordneten Datenverarbeitungsstelle (16) ausgehend nach Autorisierung eines Zugangsberechtigten gegenüber der Datenverarbeitungsstelle (16) über die Netzwerkverbindung (4) erfolgt.

Figur 1

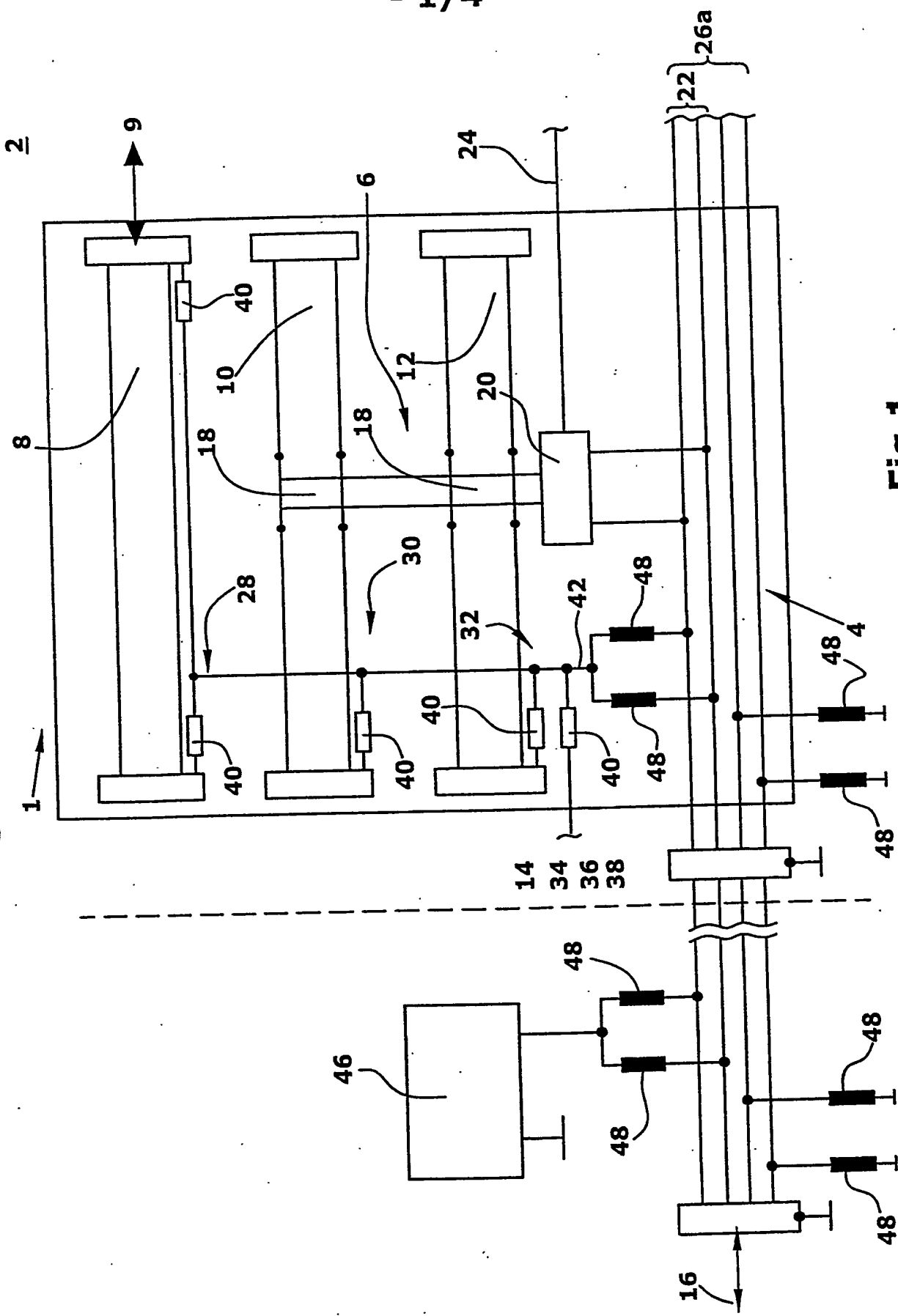


Fig.1

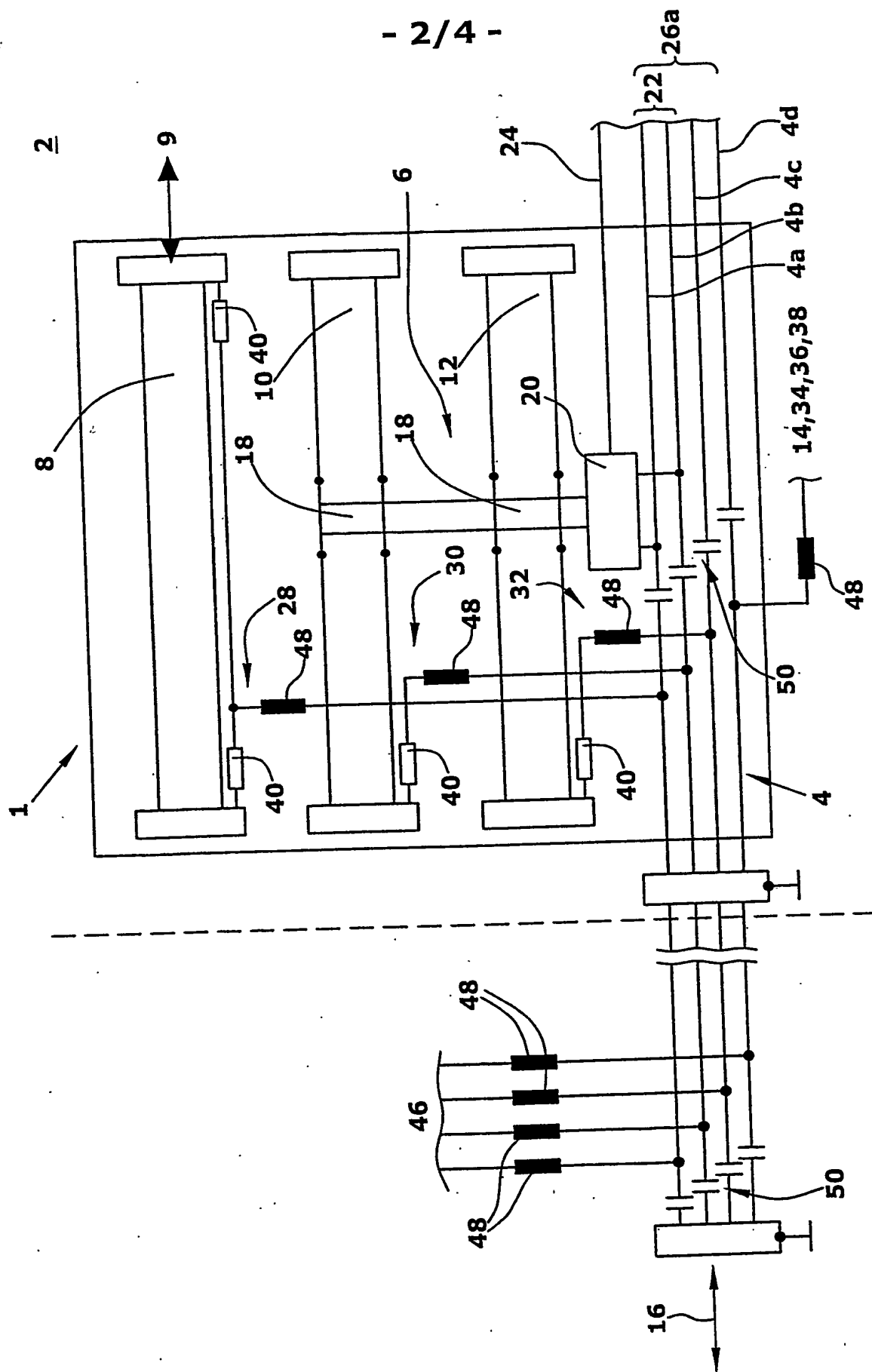


Fig.2

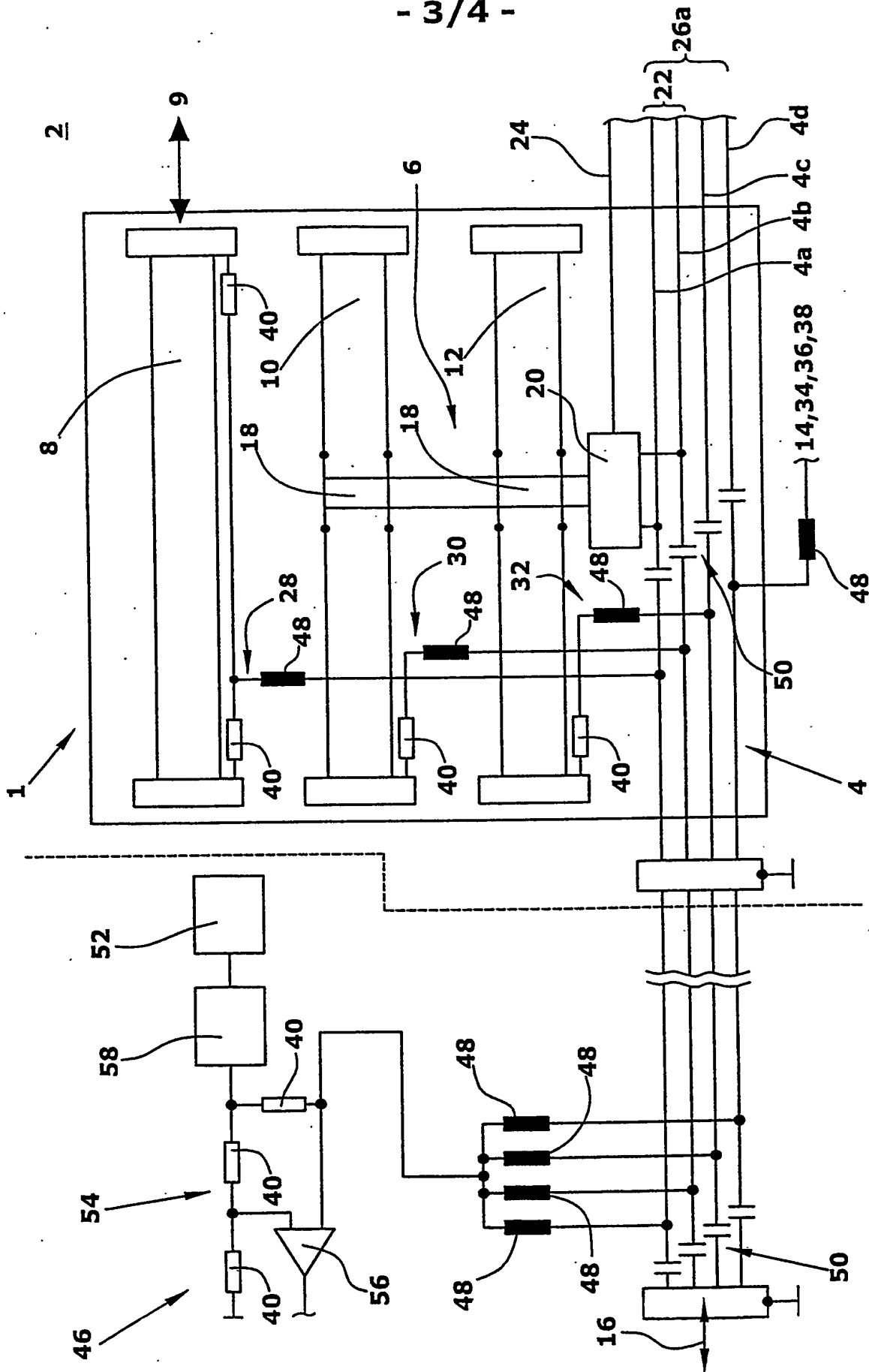


Fig.3

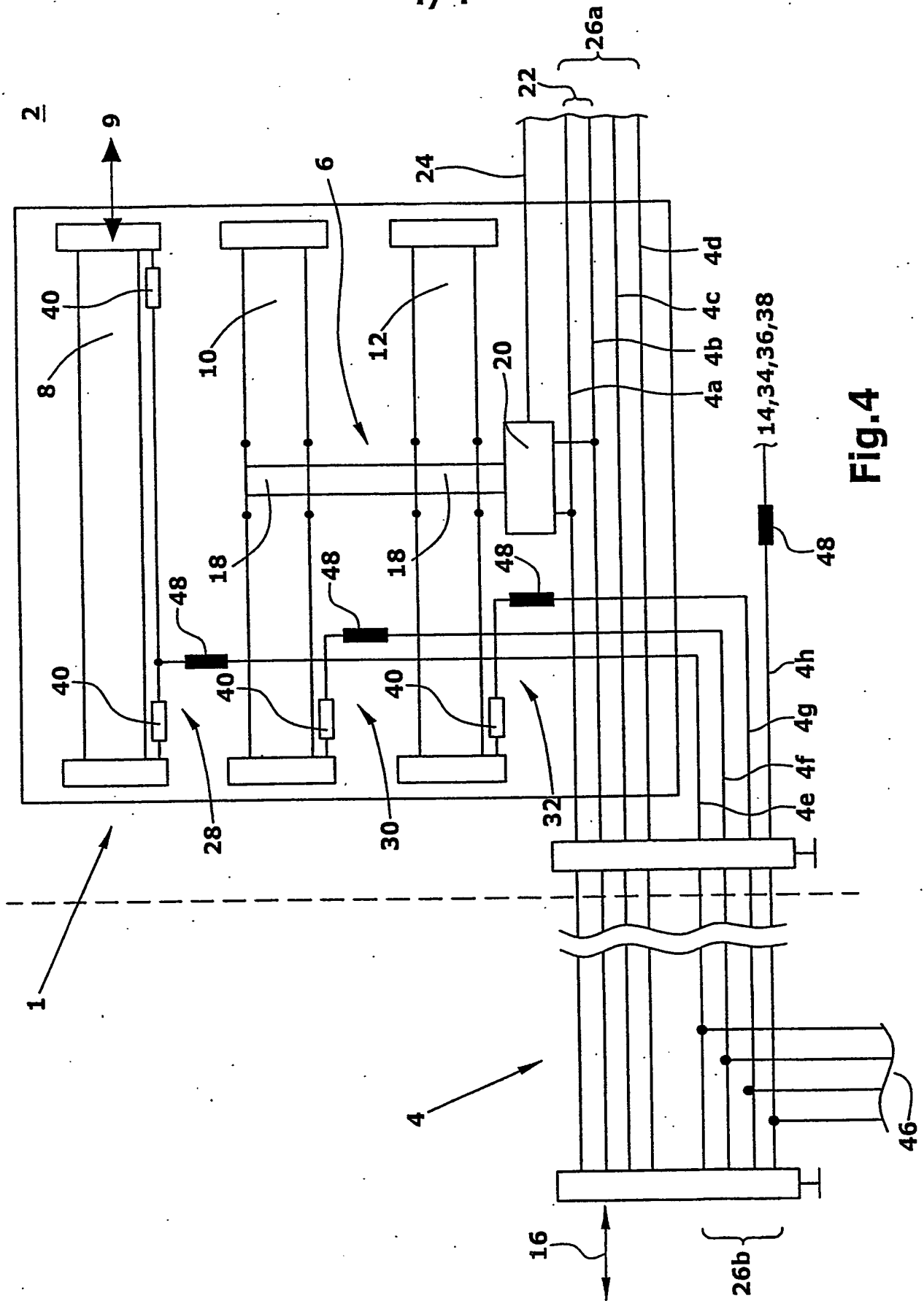


Fig.4

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.